



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/827,008 | 04/05/2001 | Richard M. Mathis | 20804.00400 | 4898 |

7590 05/24/2005

Tobi C. Clinton
CROSBY, HEAFEY, ROACH & MAY
P.O. Box 7936
San Francisco, CA 94120-7936

| |
|----------|
| EXAMINER |
|----------|

TSAI, SHENG JEN

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2186

DATE MAILED: 05/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/827,008

Applicant(s)

MATHIS, RICHARD M.

Examiner

Sheng-Jen Tsai

Art Unit

2186

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 06/04/2001.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are presented for examination in this application (09,827,008) filed on April 5, 2001.

Acknowledgement is made to the Information Disclosure Statement received on June 4, 2001.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 8 and 33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claims 8 and 33 recite "the step of disabling reading and writing of the program memory chip comprises maintaining control device stability." It is not clear what constitutes "maintaining control device stability," and how the control stability can be maintained.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 6-7, 10-14, 16-19, 26-29, 31-32, and 35 are rejected under 35

U.S.C. 102(e) as being anticipated by Charron (US 6,732,274).

As to claim 1, Charron discloses **a method of protecting a program memory device including program memory content** [Electronic Apparatus Comprising a memory Protection Device and method of Protecting Data in a memory (title)], **wherein the program memory content is associated with a previously stored signature** [a signature (a random number) is stored as a personality data in a memory (abstract; column 15, claim 1)], **the method comprising:**

automatically disconnecting [normally when the device is switched on, the control device (the electronic circuit, figure 1, 15) is prohibited from interacting with the EEPROM (the program memory device) until the signature verification is confirmed (column 3, lines 40-50; figure 4). Hence the program memory and the control device are essentially disconnected from each other] **the program memory device** [the EEPROM, figure 1, 28] **from a control device** [the electronic circuit, figure 1, 15] **that is operationally dependent upon the program memory device** [the operations of the electronic circuit as well as the entire apparatus (a mobile radio telephone station) depend on the content of the EEPROM];

halting the control device [normally when the device is switched on, the control device (i.e., the electronic circuit) is prohibited from interacting with the EEPROM (the

program memory device) until the signature verification is confirmed (column 3, lines 40-50; figure 4));

verifying whether a present signature is equivalent to the previously stored signature to obtain a verification result [(column 3, lines 40-50; figure 4)]; and based on the verification result, performing one of [(column 3, lines 40-50; figure 4)]:

disabling reading and writing of the program memory device [if the values are different, box K18 is proceeded to which stops the process of switch-on (column 3, lines 40-50; figure 4)]; or

automatically reconnecting the program memory device to the control device [if the values are identical, the apparatus operates as it should be (column 3, lines 40-50; figure 4)].

As to claim 2, Charron discloses that **the step of verifying comprises:**

independently computing a binary content verification of the program memory content [determining the digital value supplied by the generator (column 3, lines 40-50; figure 4, step K10); Charron further teaches, via referencing Brunner (US 4,727,544), a signature encoding method that determines the personality data (signature) consisting of determining a checksum based on the contents of the memory to be protected (column 1, lines 26-39)] ; and

comparing the previously stored signature with the binary content verification [(column 3, lines 40-50; figure 4)].

As to claim 3, Charron discloses that **the step of independently computing the binary content signature comprises storing the binary content signature in a secure memory device** [the digital value of the signature is written to a location in the EEPROM (column 3, lines 35-39)].

As to claim 4, Charron discloses that **the secure memory device is a securely enclosed unit that is tamperproof and that has electrical connections available for connection with the program memory device** [the apparatus (i.e., the security memory device) is enclosed in a portable radio mobile station (column 1, lines 15-20; column 2, lines 45-60); figure 1].

As to claim 6, Charron discloses that **the protecting is performed automatically and without manual intervention** [the user does not notice a thing (column 3, lines 40-50; figure 4)].

As to claim 7, Charron discloses that **the protecting is performed dynamically while the program memory device is being accessed by the control device** [column 3, lines 40-50; figure 4].

As to claim 10, Charron discloses that **the step of disabling reading and writing of the program memory device comprises preventing unauthorized programming of the program memory device** [column 3, lines 6-16; column 3, lines 40-50; figure 4].

As to claim 11, Charron discloses **a method of providing security** [Electronic Apparatus Comprising a memory Protection Device and method of Protecting Data in a memory (title)] **to a consumer interactive device** [a portable radio mobile station

(column 2, lines 45-60)] **controlled by a first control device** [figure 1, the microprocessor (25), the electronic circuit (15) and the signature generator (50)], **the method comprising:**

detecting whether the first control device is substituted for a second control device [when a copy of the EEPROM is inserted into a second control device instead of the original first control device, the signature generated by the second control device will not match the original signature stored in the content of the EEPROM, hence detecting the presence of the second control device instead of the first control device (column 3, lines 6-16)];

determining whether the second control device comprises one of a secure memory device or a secure memory socket [when a copy of the EEPROM is inserted into a second control device instead of the original first control device, the signature generated by the second control device will not match the original signature stored in the content of the EEPROM, hence detecting the presence of the second control device instead of the first control device and the mismatch of the signatures indicates that the second control device is not a security memory device associated with the EEPROM (column 3, lines 6-16)].

As to claim 12, refer to "As to claim 11." Further, Charron teaches that if the signature values are different, box K18 is proceeded to which stops the process of switch-on (column 3, lines 40-50; figure 4).

As to claim 13, refer to "As to claim 11."

As to claim 14, Charron teaches that the digital value of the signature is initially written to a location in the EEPROM by the microprocessor when used for the first time (column 3, lines 35-39).

As to claim 16, Charron discloses a **secure memory device** [figure 1] **comprising:**
an electrically accessible memory [EEPROM, figure 1, 28] **configured to store a binary image of a program memory device** [figure 2] **in communication with a control device** [the microprocessor, figure 1, 25], **wherein the control device controls computational operations of a consumer interactive device** [a portable radio mobile station, column 2, lines 45-60]; **and**
a tamperproof construction configured to detect altering of the binary image [column 3, lines 6-16; column 3, lines 40-50; figure 4].

As to claim 17, refer to "As to claim 2."

As to claim 18, Charron discloses that **the secure memory device is electrically accessible only to a program memory device connection** [figure 1].

As to claim 19, Charron discloses that **the tamperproof construction is further configured to initiate operations to disable reading and writing of the program memory device and to disable operation of the consumer interactive device** [column 3, lines 40-50; figure 4].

As to claim 26, refer to "As to claim 1." Further, figures 3 and 4 show the flowcharts of the programs for performing the memory protection.

As to claim 27, refer to "As to claim 2."

As to claim 28, refer to "As to claim 3."

As to claim 29, refer to "As to claim 4."

As to claim 31, refer to "As to claim 6."

As to claim 32, refer to "As to claim 7."

As to claim 35, refer to "As to claim 10."

6. Claims 11-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Habib (US 6,035,368).

As to claim 11, Habib discloses **a method of providing security** [Protection Method against EEPROM-Directed Intrusion into a Mobile Communication Device That Has a Processor, and a Device Having Such Protection Mechanism (title)] **to a consumer interactive device** [a mobile communication device (column 1, lines 8-40)] **controlled by a first control device** [figure 1, the micro-controller (44)], **the method comprising:**

detecting whether the first control device is substituted for a second control device [the corresponding second controller is the external device (figure 1, 48); the invention is based on having the microprocessor detecting the power-up situation, in combination with the appearance of an external master on the interface (column 1, lines 57-62); column 3, lines 59-67; column 4, lines 1-4];

determining whether the second control device comprises one of a secure memory device or a secure memory socket [the detector must distinguish between wanted and unwanted masters (i.e., a secure memory device or not) (column 3, lines 59-67; column 4, lines 1-4)].

As to claim 12, Habib teaches that the detector must distinguish between wanted and unwanted masters (i.e., a secure memory device or not) (column 3, lines 59-67; column 4, lines 1-4).

As to claim 13, Habib teaches that, under standard operating condition, the master station of the interface should be the microprocessor (figure 1, 44) itself (column 1, lines 58-62). Note that the microprocessor is the first control device as explained in "As to claim 11."

As to claim 14, Habib teaches calculating a signature of the EEPROM using encryption to protect against illegal copying (column 1, lines 29-32). Further, Habib also teaches that checking the information format from the EEPROM corresponds to expectation (column 3, lines 28-58).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 5, 20-22, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Charron (US 6,732,274).

As to claim 5, Charron does not teach that **the binary content signature is a binary bit-for-bit copy of the program memory content of the first time period,**

and the binary content verification is another binary bit-for-bit copy of the program memory content of the second time period, although Charron does teach that a checksum based on the contents of the memory to be protected may be calculated to provide the binary content signature (column 1, lines 26-39). Further, it is well known that the utilization of a signature such as a checksum is to save the storage space needed for the signature by avoiding storing the entire contents of the memory to be protected. On the other hand, a binary bit-by-bit copy of the program memory content, although requires a much larger storage space compared to a checksum, represents the utmost and the best duplication of the original information as far as verification is concerned. Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Applicants' invention to recognize the advantage of using a binary bit-by-bit copy of the program memory content as a basis of content verification, and to incorporate it as an additional option into the existing scheme disclosed by Charron to further improve the accuracy of the content verification.

With respect to claims 20-22, Charron do not mention the use of a secure memory socket. However, Charron do teach the construction and operations of a security memory device, as according to claims 16-19; and the scope of claims 20, 21 and 22 are the same as those of claims 16, 18 and 19, respectively, except for the replacement of the program memory device by a corresponding socket. Further, it is understood by one of ordinary skill in the art that a socket is a device commonly employed on electronic products to facilitate the flexibility and easiness of swapping chips in and out of a product. Therefore, it would have been obvious for ones of

Art Unit: 2186

ordinary skills in the art at the time of Applicants' invention to recognize the nature and benefits of a socket, and the mere replacing of a program memory chip by a socket is patentable insignificant, hence lacks patentability.

As to claim 30, refer to "As to claim 5."

9. Claims 9 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Charron (US 6,732,274), and in view of Schlotter et al. (US 3,827,029).

With respect to claims 9 and 34, Charron does not teach that **the method of claim 1, further comprising: disabling reading and writing of a first portion of the program memory device; and**

maintaining a second portion of the program memory device in an active state.

However, Schlotter et al. disclose in their invention "Memory and Program Protection System for a Digital Computer System" a memory protect subsystem by defining a memory region to be protected and any attempt to access the data within the protected region is disabled while attempts to access the data outside the protected region are allowed to proceed [column 3, lines 3-15; column 4, lines 3-28]. A memory protection system that disables accessing to one region while permitting accessing to another allows the system continues to perform certain functions based on the active memory space (e.g., the operating system) while protecting vital data storing in the disabled region, as demonstrated by Schlotter et al. Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Applicants' invention to recognize the benefits such a scheme, and to incorporate it into the existing system disclosed by Charron to further enhance the performance of the system.

10. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Charron (US 6,732,274), and in view of Brunner (US 4,727,544).

With respect to claim 15, Charron does not teach that the consumer interact device is one of: a gaming apparatus; a slot machine; an automatic teller machine; currency acceptor; or vending apparatus. However, the apparatus and method of Charron is readily adapted to be incorporate into these machines. Further, Brunner et al. teach in their invention "memory Integrity Checking System for a Gaming Device" a system for continuously checking the integrity of the memories of a gaming apparatus (abstract; figure 1). Charron's memory protection scheme, in addition to the checksum verification method taught by Brunner et al., would further enhance the memory security and integrity of a gaming apparatus. Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Applicants' invention to recognize the benefits offered by the memory protection scheme disclosed by Charron and to applied to the memory integrity measurements of a gaming apparatus, as illustrated by Brunner et al., to further enhance the integrity of the memory system.

11. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Habib (US 6,035,368), and in view of Brunner (US 4,727,544).

With respect to claim 15, Habib does not teach that the consumer interact device is one of: a gaming apparatus; a slot machine; an automatic teller machine; currency acceptor; or vending apparatus. However, the apparatus and method of Habib is readily adapted to be incorporate into these machines. Further, Brunner et al. teach in their invention "memory Integrity Checking System for a Gaming Device" a system for

continuously checking the integrity of the memories of a gaming apparatus (abstract; figure 1). Habib's memory protection scheme, in addition to the checksum verification method taught by Brunner et al., would further enhance the memory security and integrity of a gaming apparatus. Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Applicants' invention to recognize the benefits offered by the memory protection scheme disclosed by Habib and to applied to the memory integrity measurements of a gaming apparatus, as illustrated by Brunner et al., to further enhance the integrity of the memory system.

12. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schlotter et al. (US 3,827,029), and in view of Brunner (US 4,727,544).

As to claim 23, Schlotter et al. disclose **a method of monitoring execution of a program memory** [Memory and Program Protection System for a Digital Computer System (title)], **wherein the program memory is accessed by a controlling program of a consumer interactive device** [figure 1 shows that the memory subsystem (104) may be accessed by a plurality of controllers (130~132). One of these controllers may represent a consumer interactive device], **the method comprising: determining bounds of a contiguous block of memory accessible by the controlling program** [the addressing signals are compared to upper and lower bounds of the protected memory range (column 4, lines 3-28)]; **monitoring addresses accessed by the controlling program during execution of the controlling program to determine actually accessed addresses** [column 3, lines 4-15; column 4, lines 3-28]; **and**

determining whether the actually accessed addresses are outside the bounds of the contiguous block of memory [column 3, lines 4-15; column 4, lines 3-28].

With respect to claim 23, Schlotter et al. do not explicitly mention that the program memory is accessed by a consumer interactive device. However, the apparatus and method of Schlotter et al. is readily adapted to support the case where one of the controllers (figure 1, 130~132). Further, Brunner et al. teach in their invention "memory Integrity Checking System for a Gaming Device" a system for continuously checking the integrity of the memories of a gaming device (abstract). Brunner et al.'s invention continuously monitors the integrity of the memories where game software and data are stored by calculating a checksum for each of the memories, and compares the calculated checksum with a respective, stored checksum value to determine if any unauthorized change has been made (column 1, lines 43-62). One of the memories stores the algorithm for calculating checksum, which should never be accessed by any entity except the CPU (figure 2, 24). The memory protection scheme disclosed by Schlotter et al. would further enhance the integrity of the memory by preventing other controllers (e.g., the display controller, figure 2, 44) from accessing the memory storing the checksum algorithm. Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Applicants' invention to recognize the benefits offered by the memory protection scheme disclosed by Schlotter et al. and to applied to the memory integrity measurements of a gaming device (i.e., a consumer interactive device), as illustrated by Brunner et al., to further enhance the integrity of the memory system.

As to claim 24, Schlotter et al. and Brunner et al. teach that **the method of claim 23, further comprising:**

determining that the actually accessed addresses are outside the bounds of the contiguous block of memory [Schlotter et al., column 3, lines 4-15; column 4, lines 3-28];

disabling reading of the program memory [Schlotter et al., column 3, lines 4-15; column 4, lines 3-28]; **and**

disabling operation of the consumer interactive device [Brunner et al., for examples, enable or disable the coin input mechanism or to turn on or off the coin hopper (column 3, lines 25-65)].

As to claim 25, Schlotter et al. teach that the method is performed dynamically while the controlling program is in use [Schlotter et al., column 3, lines 4-15; column 4, lines 3-28].

13. *Related Prior Art*

The following list of prior art is considered to be pertinent to applicant's invention, but not relied upon for claim analysis conducted above.

- Martin, (US 5,729,212), "Gaming Device Providing High Security Communications with a Remote station."
- Wess et al., (WO 98/52664), "Gaming Device Security System: Apparatus and Method."
- Olarig et al., (US 6,009,524), "Method for the Secure Remote Flashing of a BIOS Memory."

- Mattison, (US 5,778,070), "Method and Apparatus for Protecting Flash Memory."
- Cragon et al., (US 3,573,855), "Computer memory Protection."

Conclusion

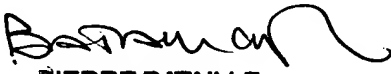
14. Claims 1-35 are rejected as explained above.
15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sheng-Jen Tsai whose telephone number is 571-272-4244. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew Kim can be reached on 571-272-4182. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sheng-Jen Tsai
Examiner
Art Unit 2186

May 20, 2005


PIERRE BATAILLE
PRIMARY EXAMINER
5/23/05